UNITED STATES PATENT APPLICATION

FOR

A LOCATION SENSITIVE WEB SERVER SYSTEM

INVENTORS:

Deborah L. Caswell

Jeffrey A. Morgan

Venkatesh Krishnan

Prepared by:

Thomas X. Li (Reg. No. 37,079)
Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Mail Stop 35
Fort Collins, CO 80527-2400
(650) 857-5972
thomas_li@hp.com

Attorney's Docket No. 10001097-1

A LOCATION SENSITIVE WEB SERVER SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention pertains to creating a web representation for a physical entity. More particularly, this invention relates to a location sensitive web server system that provides location-dependent or location-sensitive web services.

2. Description of the Related Art

As we know, the world we live in is a physical world that is formed by physical entities such as people, places, and things (or objects). For example, a bookstore is a place. So is a museum, an exhibition hall, a conference room, or a home. A book in a bookstore or a painting in a museum or exhibition hall is a thing. Likewise, a TV is a thing. A bus stop can be referred to as a place. These are some examples of physical entities.

With the rapid growth of the Internet and widespread use of the World Wide Web (WWW), more and more physical entities now have their own web sites and/or web pages. This form of representation for the physical entities is typically referred to as non-physical or virtual representation. In this case, each physical entity can have one or more web pages. In addition, each web page can also represent one or more physical entities. These web pages use written text, audio, video, and/or images to describe or illustrate their respective physical entities. The web pages may also provide services (e.g., e-commerce) for their physical entities. A person can simply go to the web pages of a

physical entity to get information about the physical entity, or to conduct business transaction with the physical entity (i.e., on-line transaction or e-commerce). These web pages form the virtual world or cyberspace of the physical world.

The web representation allows the physical entities to become more useful, convenient, and accessible. For example, instead of physically posting, at a particular bus stop, the arrival and departure schedules of various buses at that particular bus stop, the bus stop is equipped with its own web page which lists all the arrival and departure times so customers can access the information anywhere and anytime so long as they have the web address of the web page. The web page is also automatically updated in real time, thus avoiding the need for the employees of the bus company to physically post any change of the posted schedule. This provides people with accurate information cost-effectively and efficiently. As a further example, a retail store may have a web page that describes the merchandise it offers, directions to the store, and store hours. The web page might also provide easy email access for asking questions. Some stores might offer on-line ordering through their web pages.

However, although a physical entity in real world may have its web-based representation, the two are not tightly connected. This means that there is no means for bridging the two worlds together. In other words, the prior art structure does not provide means for linking people who are accessing a physical entity to its web page. For a person to find the right web page of a physical entity, the person either has to memorize the web address of the web page, or has to find the web page through searching and browsing the Web. This causes difficulty and inconvenience for the users to access those web

pages. The inconvenience has increasingly become obvious because the Web has now grown to contain millions of millions of web sites and/or web pages. In addition, web pages are typically within a web site. The address of a web site is relatively short and easy to remember. For example, the address of the web site of Hewlett-Packard Company is "www.hp.com" while the address of the web site for Microsoft Corporation is "www.microsoft.com". However, this is not the case for the address of a web page within a web site. For example, the address of the web page for a particular turtle neck sweater on the Gap Inc's web site may be "www.gap.com/onlinestore/gapstore/product.asp?wpid=12977&sid=7HWUHNGFFSS12H0B00AKH2QFP8FE1BP4&wdid=214". This is very hard to remember and use. The reason that the address is so long and confusing is that these web pages are transient and can be changed on a regular basis because physical inventory changes rapidly.

In addition, the prior web server system that hosts the web sites or web pages for the physical entity cannot distinguish user access requests that are generated by the users at the physical location of the physical entity from other user access requests that are generated by the users not at the physical location. This means that the web server system does not take into consideration where the user accesses the web server for the physical entity . There are many ways that the user can obtain the web address of the physical entity and then access the web server for the physical entity. For example, the user can sit at home or office searching through various search engines to obtain the web address. In this case, the user access is a remote one. As a further example, the user may be at the location of the physical entity and see the web address posted there. Then

the user accesses the web server at the very location of the physical entity. Because the prior web server system does not distinguish user access requests based on their location, the web server system cannot provide special information and/or service to users accessing the web server at the physical location. Often times, there exists a need for the web server system to know this information and to provide different information and/or services based on this information. However, no existing prior art technology is able to solve this problem.

The above-mentioned problems are also amplified by the fact that more and more people can now access the Web through their mobile electronic devices. As we know, with the increased availability of highly functional portable or mobile devices and development of wireless networking options, more and more people are always connected to the Web through their mobile browser, no matter where they are.

SUMMARY OF THE INVENTION

One feature of the present invention is to allow easy and quick web services that are location sensitive or location-dependent.

Another feature of the present invention is to provide a location sensitive or location-dependent web representation and/or service for a physical entity.

A further feature of the present invention is to provide a location sensitive web access system for a physical entity that provides different services to users based on the users' relative positions or locations with respect to the physical entity.

A location sensitive web server system for a physical entity includes a location beacon located adjacent to the physical entity. The location beacon transmits a beacon signal containing (1) a web address of a web site for the physical entity and (2) a location token that expires within a predetermined time period. The beacon has a predetermined transmission range. The system also includes a web server that hosts the web site for external accesses with the web address. The system also includes a location authentication module that causes the web server to restrict access to the web site if an access request does not contain the location token or the location token has expired.

A location sensitive web server system for a physical entity includes a web server that generates content regarding or related to the physical entity in response to external requests with the web address of the web server. A location beacon is located adjacent to the physical entity to transmit a beacon signal containing (1) the web address of the web server and (2) a location token that expires within a predetermined time period. The location beacon has a

predetermined transmission range. A location authentication module causes the web server to provide (1) a first version of web content if an external request does not contain the location token or the location token has expired, or (2) a second version of web content if the external request contains the location token that has not expired.

Other features and advantages of the present invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, illustrating by way of example the principles of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a location sensitive web server system for a physical entity that implements one embodiment of the present invention, wherein the location sensitive web server system provides different services to users accessing the web server system based on their locations.

Figure 2 shows the structure of the location beacon of the web server system of Figure 1.

Figure 3 shows the flow chart diagram of the location authentication process of the location authentication module of the web server system of Figure 1.

Figure 4 shows the flow chart diagram of the content generating process of the content generator of the web server system of Figure 1.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 shows a location sensitive web server system 20 that implements one embodiment of the present invention. The location sensitive web server system 20 provides a web representation for a physical entity 11. The web representation may include web content pages and/or services (e.g., on-line conference room booking or scheduling, e-commerce). Figure 1 also shows a mobile client system 30 that can access the location sensitive web server system 20 via global Internet 40.

As will be described in more detail below, the location sensitive web server system 20 provides a location sensitive web content and/or service for the physical entity 11. This means that when the location sensitive web server system 20 receives a user access request, it determines whether the user access request was generated from a client device/system *close to* the physical entity 11. A client system is a device that contains a web browser for accessing remote web server systems via Internet (i.e., the global Internet 40). Here, the term "*close to*" means that the client system can be within, near, or adjacent to the physical entity 11.

If the access request is generated from a client system adjacent to the physical entity 11, the web server system 20 provides one type or form of web contents and/or services to the requesting client device. If the client system is not near or adjacent to the physical entity 11 when generating the access request, the web server system 20 provides another type or form of web contents and/or services to the requesting client device. For example, if the physical entity 11 is a conference room, the first type or version of web contents

that the web server system 20 can offer a link to control the conference room's projector while the second type or version of web contents can simply be web pages describing and/or showing the conference room. As a further example, if the physical entity 11 is an exhibition hall, the first type of web contents that the web server system 20 can provide can be web pages describing and/or showing the layout of the exhibition hall and various services (e.g., food, gift shops, post office, banks, ATM machines, etc.) provided inside the hall while the second type of web contents can simply be web pages that provide general description of the exhibition hall (e.g., direction, hours, address, and contact information, etc.).

The location sensitive web server system 20 accomplishes or achieves this by placing or locating a location beacon 23 adjacent to the physical entity 11. The location beacon 23 transmits a beacon signal that contains the web address of the web server system 20 for the physical entity 11 and a location token that expires within a predetermined time period. The location token is generated with a secret key uniquely identified with the physical entity 11. The beacon 23 has a short transmission range so that only a client system (e.g., the client system 30) adjacent to the physical entity 11 can receive the beacon signal containing both the web address and the location token. The client system 30 can then attach the location token to its access requests to the location sensitive web server system 20. This allows the location sensitive web server system 20 to distinguish these access requests from remote access requests that are generated from client systems that are not adjacent to the physical entity 11.

In addition, the location sensitive web server system 20 includes a web

server 25 that is capable of providing different contents and/or services to an access request. The difference in the contents and/or services provided by the web server 25 depends on whether user access request contains the location token or not. Moreover, the location sensitive web server system 20 includes a location authentication module 21 that determines or verifies whether a user access request received in the web server system 20 contains the location token that has not expired.

The operation of the web server system 20 is as follows. The location beacon 23 uses a secret key stored in a secret key store 24 to generate the location token which contains a time stamp. The location beacon 23 then transmits the beacon signal containing the web address and the location token. When the client system 30 accesses the location sensitive web server system 20 with the web address, the location token is also attached to the access request which is sent to the location sensitive web server system 20. The location authentication module 21 then determines whether an access request contains the location token, and if so, to process (e.g., decrypt it with the same secret key stored in the secret key store 24) the location token to expose the time stamp in the token.

If the location authentication module 21 determines that the access request does not contain any valid location token (i.e., no location token or the location token has expired), then the location authentication module 21 causes the web server 25 to provide or generate the web contents designed for access requests without the valid location token. This can be in the form of access restriction or censored web content.

On the other hand, if the location authentication module 21 determines

that the access request contains the valid location token, the location authentication module 21 causes the web server 25 to provide or generate the web contents designed for access requests with the valid location token. This can be in the form of unrestricted access or uncensored web content. The location sensitive web server system 20 will be described in more detail below, also in conjunction with Figures 1 through 4.

Referring again to Figure 1, the web server 25 of the web server system 20 represents the physical entity 11 in the virtual world by the contents contained in the web server 25. Here, the physical entity 11 can be a person, a place, or a thing/object. This means that the physical entity 11 can be a bookstore, a museum, a conference room, or a hotel room. The physical entity 11 can also be a convention center, a bus terminal or stop. Moreover, the physical entity 11 can be a book in a bookstore, a painting in a museum, an item on display in an exhibition hall or convention center.

The web representation of the physical entity 11 by the web server 25 means that the web server 25 contains or generates information and/or services related to the physical entity 11. The web representation also means that the web server 25 may also contain or generate written text, audio, video, and/or images to describe the physical entity 11. For example, if the physical entity 11 is a car in an exhibition hall, the web server 25 can generate a list of all the features of the car. It may also include some audio information about the car. Moreover, two-dimensional or three-dimensional images may also be included to illustrate the internal structure of the car. The web server 25 may also contain or generate video programs about the car. The web server 25 can also allow on-line order of the car. In this case, the customer may actually order a custom-

built car of the same brand. As a further example, when the physical entity 11 is a conference room, the web contents can be (1) the on-line conference room booking services, and/or (2) web pages describing and/or showing the conference room. If the physical entity 11 is an exhibition hall, the web contents can be web pages describing and/or showing the layout of the exhibition hall and various services (e.g., food, gift shops, post office, banks, ATM machines, etc.) provided inside the hall, and/or the web pages that provide general description of the exhibition hall (e.g., direction, hours, address, and contact information, etc.).

The web server 25 includes a HTTP engine 26 and a content generator 27. The HTTP engine 26 receives and handles access requests to the web server system 20. The access requests are sent to the web server system 20 from various client systems via the global Internet 40. Here, the global Internet 40 means the Internet that people now know. This means that an open standard transmission protocol is used to transmit the access requests. In one embodiment, the open standard communication protocol is the HTTP (Hyper Text Transport Protocol) protocol. Alternatively, other open standard communication protocols may be used.

Here, an access request to the web server system 20 typically includes some or all of the following data items, although not necessarily in the order described below. The order of the data items is to facilitate the description of the present invention only. The first data information is the web address of the web server system 20. The web address helps direct the address request to the HTTP engine 26 of the web server system 20 via the global Internet 40. The second data information of the access request is the IP (Internet Protocol)

address of the access request. The IP address uniquely identifies the origin of the access request. This means that the IP address identifies from which user terminal or client system the access request is generated. The third data information of the access request is the arguments and/or parameters that specify what response the web server 25 should provide or generate to the access request.

The fourth data information contained in the access request is the location token. If the client system that generates the access request receives the web address of the web server system 20 near the location beacon 23, then the web address received is also attached with a location token. The location token is an encrypted token and contains a time stamp. The token, when generated, is a series of numbers. A secret key is used to generate the location token as well as decrypt the token in the web server system 20. The secret key is stored in a secret key store 24. The use of the secret key to encrypt and decrypt the location token is to prevent any possible tampering with the time stamp contained in the location token. The access request may contain more or less data information than the above mentioned ones.

In one embodiment, the location token is contained in a cookie that is attached to the HTTP access request. In another embodiment, the location token is not contained in a cookie, but is directly attached to the access request.

As described above, the HTTP engine 26 receives and handles access requests to the web server system 20. The engine 26 also sends responses to these access requests back to their respective requesting client systems. These functions of the HTTP engine 26 are known and will not be described in more detail below.

In accordance with one embodiment of the present invention, the HTTP engine 26 includes the function of separating the location token from the access request when handling or processing the access request. This means that if the HTTP engine 26 receives an access request that contains a cookie that contains the location token, the engine 26 separates the location token from the cookie. The engine 26 does this by separating the data field reserved for the location token from the cookie or from the access request itself using any known technique. The data contained in this particular data field is the encrypted location token, which is then sent to the location authentication module 21.

The access request, once processed by the HTTP engine 26, is sent to the content generator 27 of the web server 25. The main function of the content generator 27 is to provide or generate web contents regarding or related to the physical entity 11. As described above, the web contents contained or generated can be web content pages, application programs, and/or a combination thereof. The application programs can be e-commerce application programs that provide e-commerce services. The application programs can be other types of application programs such as on-line conference room booking or scheduling. The application programs can also be content generating programs that can generate web content pages on-the-fly based on parameters and/or arguments in the access requests.

In accordance with one embodiment of the present invention, the content generator 27 is capable of providing or generating different types of web contents for access requests with the same IP address (i.e., coming from the same client system). For example, if the physical entity 11 is a conference room, the content generator 27 can provide or generate on-line conference room

booking and billing services as well as web pages describing and/or showing the conference room. As a further example, if the physical entity 11 is an exhibition hall, the content generator 27 can provide or generate web pages describing and/or showing the layout of the exhibition hall and various services (e.g., food, gift shops, post office, banks, ATM machines, etc.) provided inside the hall, as well as web pages providing general description of the exhibition hall (e.g., direction, hours, address, and contact information, etc.). Which type of web contents the content generator 27 is to provide is controlled by the location authentication module 21, thus making the web server system 20 a location sensitive web server system. This will be described in more detail below.

The location authentication module 21 is used to validate the location token received from the HTTP engine 26. First, the location authentication module 21 determines if a location token is received. If so, the location authentication module 21 decrypts the location token using the secret key stored in the secret key store 24. As described above, the secret key is used to generate the location token. The decryption will expose the time stamp contained in the location token. The time stamp is embedded into the location token when the token was first generated. The time stamp indicates the time at which the location token expires (based on the time at which the location token was generated plus the valid time duration or interval). The duration is on the order of minutes and is chosen for its specific use. The location authentication module 21 then determines whether the location token has expired by comparing the time stamp with the current time.

If the location authentication module 21 determines that no location token is received or if the received location token has expired, then the location

authentication module 21 controls the content generator 27 to generate or provide the web contents designed for access requests generated from remote client systems. This can mean restricted access to the content generator 27 or censored contents. If, on the other hand, the location authentication module 21 determines that location token is valid and unexpired, then the location authentication module 21 controls the content generator 27 to generate or provide the contents designed for access requests generated from client systems that are adjacent to the physical entity 11. In this case, the web contents can be unrestricted access or uncensored contents. Figure 3 shows the operation of the location authentication module 21, which will be described in more detail below.

Referring again to Figure 1, the location beacon 23 is used to store and transmit the beacon signal that contains the web address (i.e., URL) of the web server system 20 and the location token. Although the physical entity 11 might be physically separated from the location sensitive web server system 20, the location beacon 23 is located or placed adjacent to the physical entity 11. Here, the term "*adjacent to*" means that the location beacon 23 can be placed or located on, in, around, or near the physical entity 11. For example, if the physical entity 11 is a small object (e.g., a car or a painting in a museum), the location beacon 23 can be placed near or on the object. If the physical entity 11 is a place (e.g., a conference room or museum), the location beacon 23 can be placed in the front of the place or inside the place. In essence, the location beacon 23 can be treated like a poster. Alternatively, the entire web server system 20 is located or placed adjacent to the physical entity 11.

Figure 2 shows the structure of the location beacon 23. As can be seen from Figure 2, the location beacon 23 includes a token generator 40, a store 41,

and a communication interface 46. The communication interface 46 is used to broadcast or transmit the beacon signal in accordance with a predetermined open standard communication protocol. The communication interface 46 can be implemented using any known wireless communication means that broadcasts or transmits signals (referred to as beacon signal). In one embodiment, the communication interface 46 constantly transmits the beacon signal. In another embodiment, the communication interface 46 periodically transmits the beacon signal. Alternatively, the communication interface 46 transmits the beacon signal whenever activated by external stimulus.

The transmission range of the communication interface 46 is determined by the communication technology adopted by the communication interface 46. In one embodiment, the communication technology employed by the communication interface 46 can be a short range wireless technology such as infrared (e.g., the IrDA technology developed by several companies including Hewlett-Packard Company of Palo Alto, California), ultra-sound, or the low power, high frequency, short-range radio (2.4 - 5 Ghz) transmission (e.g., the Bluetooth technology developed by several telecommunications and electronics companies).

In one embodiment, the communication interface 46 has a transmission range of approximately three to six feet. Alternatively, the transmission range of the communication interface 46 can be shorter than three feet or longer than six feet. In one embodiment, only the communication interface 46 is placed or located adjacent to the physical entity 11. In another embodiment, the entire location beacon 23 is placed or located adjacent to the physical entity 11.

The store 41 includes a URL store 43 and a token store 44. The URL

store 43 stores the web address of the web server system 20 (Figure 1). The token store 44 stores the location token. Each of the stores 43-44 can be electronically updated with new information. Each of the stores 43-44 can store information volatilely or non-volatilely. An interface 42 is used to supply data to each of the stores 43-44.

Each of the stores 43-44 stores a predetermined amount of data. In one embodiment, the URL store 43 can store 128 bytes of data. In alternative embodiments, the URL store 43 can be longer or shorter than 128 bytes. The web address stored in the URL store 43 can be in various forms. In one embodiment, the web address stored in the URL store 43 is already decoded into the binary form. In another embodiment, the web address stored is in the "name=value" pair form (i.e., the Extensible Markup Language (XML) form). Alternatively, the web address stored in the URL store 43 can be in other forms (e.g., WML form). In addition, the URL store 43 can store more information than just the web address.

In one embodiment, the token store 44 can store 128 bytes of data. In alternative embodiments, the token store 44 can be longer or shorter than 128 bytes.

The location beacon 23 also includes a token generator 40. The token generator 40 receives a date and time signal and the secret key from the secret key store 24 (Figure 1). The token generator 40 generates the location token. This location token is essentially a time stamp. Then the location token is encrypted using the secret key. In one embodiment, the encryption is done using any known symmetric encryption technology. In another embodiment, the encryption is done using any known asymmetric encryption technology. In this

case, different keys are used to encrypt and decrypt the location token. The encryption is to prevent user tampering of the time stamp in the location token. The encrypted token is then sent to the token store 44 via the interface 42.

The token generator 40 periodically generates a new location token. This means that each location token generated has a different time stamp. In one embodiment, the token generator 40 generates a new location token in every two minutes. In another embodiment, the token generator 40 generates a new location token in every ten minutes.

Referring back to Figure 1, the operation of the location sensitive web server system 20 is now described. During operation, the location beacon 23 transmits the beacon signal that contains the web address of the web server system 20 and the location token generated by the web server system 20. The location token has a time stamp. As described above, the location beacon 23 has a transmission range and is placed or located adjacent to the physical entity 11.

When a user with a client system (e.g., the client system 30) approaches the physical entity 11, the beacon signal is received by the client system 30. As can be seen from Figure 1, the client system 30 includes a beacon receiver 31, a web browser 32 and a cookie cache 33. The beacon receiver 31 allows the client system 30 to receive the beacon signal when the client system 30 is adjacent to the physical entity 11. The web browser 32 enables the client system 30 to access web servers via the global Internet 40. The web browser 32 can be any known web browser. The cookie cache 33 is used to temporarily store location token received from the location beacon 23, and to attach the location token to the access requests generated by the web browser in the form

of, for example, cookies.

The client system 30 can then generate the HTTP access request that includes the web address of the web server system 20, as well as the location token. The web address then directs the access request to the web server system 20 via the global Internet 40.

When the web server 25 receives the access request, the HTTP engine 26 separates the location token from the request and sends the location token to the location authentication module 21. The location authentication module 21 then decrypts the location token with the same secret key stored in the secret key store 24 to expose the time stamp in the token. This allows the location authentication module 21 to determine whether the location token has expired. If the location authentication module 21 determines that the access request does not contain any valid location token (i.e., no location token), or if the location authentication module 21 determines that the location token has expired, then the location authentication module 21 causes the content generator 27 to provide or generate the web contents designed for access requests from remote client systems. If the location authentication module 21 determines that the location token is valid and unexpired, the location authentication module 21 causes the content generator 27 to provide or generate the web contents designed for access requests generated by client systems that have received the unexpired location token. These client systems are local users because they would not have picked up the valid and unexpired location token had they not been within the transmission range of the location beacon 23. Since the location beacon 23 is placed or located adjacent to the physical entity 11, the web server system 20 can distinguish access requests from client systems that

are adjacent to the physical entity 11 from access requests that are generated by remote client systems that are not adjacent to the physical entity 11. This makes the web server system 20 a location sensitive web server system.

Figure 3 shows in flow chart diagram form the location authentication process of the location authentication module 21 of Figure 1. As can be seen from Figure 3, the process starts at the step 50. At the step 51, the location authentication module 21 determines whether the received data from the HTTP engine 26 contains the location token. If not, the next step is the step 57. If the answer is yes, then the step 52 is performed.

At the step 52, the location authentication module 21 receives the location token. Then the location token is decrypted using a secret key stored in the secret key store 24 to expose the time stamp in the location token at the step 53. If the location token was encrypted using a symmetric encryption technology, the secret key is the same secret key used by the location beacon 23 to generate the location token. The decryption process is the reverse process of the encryption process used by the location beacon 23 to generate the location token, and it is done using known encryption/decryption technology. Thus, the decryption process will not be described in more detail below.

At the step 54, the exposed time stamp is compared with the actual time of day to allow determination of whether the time stamp has expired. The time stamp mechanism is employed to ensure that the user at the client system 30 only generate the HTTP access request at or near the physical entity 11 both in terms of time and geographical location. In other words, the time stamp only allows the user to generate the HTTP requests with the location token shortly after receiving the location token at or near the physical entity 11. The time

stamp mechanism makes sure that the user will not just receive the web address at or near the physical entity 11 and store it for future access to the web server system 20. If the user does that, the time stamp will expire and the location token becomes invalid. The step 54 is employed to check whether the current request received in the web server system 20 contains a valid unexpired location token.

At the step 55, the determination is made. If the answer is yes which means that the location token has expired, then the step 57 is the next step. At the step 57, a denial signal is generated by the location authentication module 21. The denial signal will be used to inform the content generator 27 to only provide or generate the web contents designed for access requests that do not have the valid location token (or the token has expired).

If, at the step 55, the answer is no which means that the location token has not expired and is valid, then the step 56 is performed at which the location authentication module 21 generates an approval signal. The approval signal will control the content generator 27 to provide or generate the web contents designed for access requests that are accompanied by the valid location token. Then the process moves to the step 58, at which the signal (whether denial or approval signal) is send to the content generator 27. The process then ends at the step 59.

Figure 4 shows in flow chart diagram form the content generation process of the content generator 27 of Figure 1. As can be seen from Figure 4, the process starts at the step 60. At the step 61, the content generator 27 receives the request from the HTTP engine 26. As described above, the request received by the content generator 27 contains arguments and/or parameters that specifies

the request. At the step 62, the content generator 27 receives the approval or denial signal from the location authentication module 21. At the step 63, the content generator 27 determines whether the received signal is the approval signal or the denial signal. If the signal is the denial signal, the step 64 is performed, at which the content generator 27 provides or generates the web contents designed for remote users (i.e., for user access requests that do not contain the location token or the token contained has expired).

If, at the step 63, it is determined that the received signal is the approval signal, then the step 65 is performed, at which the content generator 27 provides or generates the web contents designed for local users (i.e., for user access requests that contain the unexpired location token). Then the web contents are sent to the HTTP engine 26. The process then ends at the step 67.

In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident to those skilled in the art that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.